SUBJECT: Change 4 to GCCS Implementation Procedure (IP) Document

1. This is Change 4 to GCCS Implementation Procedure (IP) document, dated 27 June 1997. Remove obsolete pages and destroy them in accordance with applicable security regulations. Insert new pages as indictaed below:

Remove Pages	**Insert New Pages**
vi	vi
6-26	6-26
7-7	7-7
8-1	8-1
9-1	9-1
10-1	10-1
10-3	10-3
11-2	11-2
14-3	14-3
15-1	15-1

2. These change pages become effective upon receipt.

3. When this change has been made, post an entry in the Record of Changes and file this letter before the title page.

FORWARD

IMPORTANT:

- Complete documentation may be found on the GCCS SIPRNET Web Site. The segment sizes are listed in the following order: Tape Segment size, SAINSTALLER reserved size and actual installed size, all in KBS. System Backup if installed will alter the reserved size to reflect the actual size through a CRON job. Only sites currently executing the following segments should load them. GRIS, GUPD, GORA.P1, GUPD.P1, GSORTS.P2.

- Please inform the GMC of your status prior to and after completion of your loads. A machine must be at GCCS 2.2 level before installing any server segments.

List of Tables

SECTION 6. CONFIGURING THE EXECUTIVE MANAGER SERVER

6.1 Scope

This section provides detailed instructions on configuring the GCCS Executive Manager (EM) Server. These procedures address an EM server that is also the NIS+ and Sybase server which is the GCCS recommended EM server configuration. It is not mandatory that the NIS+ and Sybase servers also be on the EM server. Section 6.8 provides instructions for creating a GCCS COE Kernel Network Installer on the EM server.

6.2 Initializing the Executive Manager Server

The GCCS Kernel version 2.2 will automatically run the "*EM_make_server*" script, which creates an EM server, when the system is rebooted after the kernel has been loaded and configured. The only time that "*EM_make_server*" script is not automatically run is when the system does not have a separate */h/data/global* partition, either local or NFS mounted. This exception was necessary to address the AGCCS SPARC 20s where the */h/data/global* partition is located on SPARCstorage arrays and is not available when the kernel is initially installed.

Verifying system as EM Server and perform the following steps:

1. Log in as **root.**

2. Execute the following:

   `/h/EM/progs/EM_mode` <**Return**>.

```
SERVER
```

3. If the system does not respond with "SERVER" execute the following:

   `/h/EM/systools/EM_make_server` <**Return**>

```
40 blocks
177 blocks
```

4. To insure that the */h/data/global* files system was correctly set up execute the following:

   `ls -l /h/data/global/EMDATA` <**Return**>

```
total 26
drwxrwx---    2 root     gccs          512 May 29 16:35 app-config
drwxrwx---    2 root     gccs          512 Jun 18 08:24 config
drwxrwx---    2 root     gccs          512 Jul 11 18:24 log
drwxr-xr-x    4 root     other         512 Jul 10 18:04 msql
drwxrwx---    2 root     gccs          512 May 29 16:35 security
drwxrwx---    2 root     gccs          512 May 30 11:40 sybase
drwxrwx---    2 root     gccs          512 Jun 25 08:41 transfer
```

6.3 Initializing the NIS+ Server

During the installation of the kernel, scripts were created to assist you in creating a NIS+ server or client. In addition you had the option of inputting data to set up the NIS+ hosts and netgroup files. All NIS+ data files are located in */etc/nis*, the NIS+ administration scripts are located in */etc/nis/admin*.

6.3.1 Verifying NIS+ Data Files Are Accurate

1. Execute the following:

   `cd /etc/nis` **<Return>**
   `more hosts` **<Return>**

```
Following is an EXAMPLE only:

164.117.210.77   alpha amhserver
164.117.210.51   facit
164.117.210.3    hardey
164.117.210.4    laurel
164.117.210.21   mobius
164.117.210.64   beta
164.117.210.65   mike
164.117.210.169  lorax
164.117.210.166  brady
164.117.210.63   martin
164.117.210.61   zeppo
164.117.210.62   zorro
```

2. Insure that all the workstations/servers in your NIS+ domain are included. If not, edit the file appropriately.

3. Execute the following to check out the passwd file:

   `more passwd` **<Return>**

```
secman:x:100:1:Security Admin:/h/USERS/secman/Scripts:/bin/csh
```

4. Insure that the entry for "*secma*n" appears exactly as shown above. If not, correct it.

5. Execute the following to check out the shadow file:

   more shadow <Return>

```
secman:sDopf20kucL2a:9654::::::
```

6. Insure that the entry for "*secman*" appears exactly as shown above. If not, correct it.

7. Execute the following to check out the netgroup file:

   more netgroup <Return>

Following is an EXAMPLE of a netgroup file:

```
allowed (alpha,-,osprey.gccs.nis.)
allowed (beta,-,osprey.gccs.nis.)
allowed (brady,-,osprey.gccs.nis.)
allowed (facit,-,osprey.gccs.nis.)
allowed (hardey,-,osprey.gccs.nis.)
allowed (laurel,-,osprey.gccs.nis.)
allowed (lorax,-,osprey.gccs.nis.)
allowed (martin,-,osprey.gccs.nis.)
allowed (mike,-,osprey.gccs.nis.)
allowed (mobius,-,osprey.gccs.nis.)
allowed (zeppo,-,osprey.gccs.nis.)
allowed (zorro,-,osprey.gccs.nis.)
```

8. Insure that the netgroup file is correct. If not, edit the file appropriately.

9. Verify the NIS+ group file is correct by executing the following:

   more group <Return>

Following is the NIS+ group file for a site where AMHS is used. If you are not using AMHS only the first two entries (gccs, admin) should appear.

```
gccs::100:secman
admin::101:secman
topic::200:
amh_cwp::201:
amh_excl::202:
amh_fbis::203:
amh_limd::204:
amh_nato::205:
amh_pers::206:
amh_spec::207:
amh_ts::208:
amh_rel::209:
```

10. Insure that the NIS+ group file is accurate. If not, edit the file appropriately.

11. In the GCCS 2.2 Kernel the networks file is being added to NIS+. Verify that it represents the EM server */etc/networks* file by executing the following:

    more networks <**Return**>

Following is an EXAMPLE of NIS+ "networks" file.

```
#ident     "@(#)networks    1.4   92/07/14 SMI"    /* SVr4.0 1.1    */
#
# The networks file associates Internet Protocol (IP) network numbers
# with network names.  The format of this file is:
#
#    network-name     network-number   nicnames . . .
#
# The loopback network is used only for intra-machine communication
#
loopback   127
#
# Internet networks
#
arpanet          10         arpa  # Historical
subnet1.gccs 164.117.210.255
```

12. Insure that the NIS+ networks file is identical to the EM servers */etc/inet/networks* file. If not, copy the */etc/inet/networks* file to */etc/nis*.

13. The automounter files (auto_home, auto_master, and auto_direct) have also been added to the NIS+ files. If you wish to add entries to them do so at this time. Examples of these files are shown below:

```
auto_master file:
# Master map for automounter
#
+auto_master
/net        -hosts           -nosuid
/home            auto_home
/-          auto_direct

auto_home file:
# Home directory map for automounter
#
+auto_home

auto_direct file:
# auto_direct directory for the automounter
+auto_direct
/usr/share/man -ro acserver:/usr/man
```

14. The "End User Support" level of the Solaris 2.3 operating system does not provide man pages. To facilitate man pages an entry has been added to the "*auto_direct*" file to automatically mount the man pages from a system that has the "Entire Distribution" loaded (usually a SPARC 1000/2000). To use this feature you must change the "**acserver**" entry in the **auto_direct** file to the hostname of the platform that is sharing */usr/man*.

15. Verify that the scripts that initialize the NIS+ server have the correct NIS+ domain and correct NIS+ server name by executing the following.

    cd /etc/nis/admin <**Return**>
    cat nis_server <**Return**>

```
#!/bin/ksh
#
#    nis_server
#
#  NIS+ domainname will replace "nisdom" when kernel is installed.

/usr/lib/nis/nisserver -r -d  osprey.gccs.nis.
#
#
/usr/lib/nis/nispopulate -F -p /etc/nis -d osprey.gccs.nis.

nischmod n+r passwd.org_dir

echo `domainname` > /etc/defaultdomain

read RETURN?'Rebooting the system to activate NIS+, hit return when
ready.'

init 6
```

16. The "**osprey.gccs.nis.**" should be replaced with the NIS+ domainname you specified when loading the GCCS COE Kernel. If not, correct it.

17. Check out the "*nis_server_post*" script by executing the following:

    more nis_server_post <Return>

```
#!/bin/ksh
#
#    nis_server_post
#
nischmod n+r passwd.org_dir

/usr/bin/nisgrpadm -a  admin.osprey.gccs.nis.
secman.osprey.gccs.nis.

su - secman -c "/usr/lib/nis/nisclient -u"
```

18. The "**osprey.gccs.nis.**" should be replaced with the NIS+ domain name you specified when loading the GCCS COE Kernel. If not, correct it.

6.3.2 Initializing the NIS+ Server

1. Execute the following to begin process of initializing NIS+ server:

   `/etc/nis/admin/nis_server` <**Return**>

```
This script sets up this machine "osprey" as a NIS+
Root Master Server for domain osprey.gccs.nis.

Domainname             : osprey.gccs.nis.
NIS+ Group              : admin.osprey.gccs.nis.
YP compatibility        : OFF
Security level             : 2=DES

Is this information correct? (Y or N)
```

2. Answer [**y**] if the information is correct and press <**Return**>.

```
This script will set up your machine as a Root Master server for
domain osprey.gccs.nis.

Use "nisclient -r" to restore your current network service
environment.
Do you want to continue? (Y or N)
```

3. Answer [**y**] and press <**Return**>.

```
setting up domain information "osprey.gccs.nis." ...
mv: cannot access /etc/defaultdomain

setting up switch information ...

running nisinit ...
This machine is in the osprey.gccs.nis. NIS+ domain.
Setting up root server ...
All done.

starting root server at security level 0 ...

running nissetup ...
org_dir.osprey.gccs.nis. created
groups_dir.osprey.gccs.nis. created
passwd.org_dir.osprey.gccs.nis. created
group.org_dir.osprey.gccs.nis. created
auto_master.org_dir.osprey.gccs.nis. created
auto_home.org_dir.osprey.gccs.nis. created
bootparams.org_dir.osprey.gccs.nis. created
cred.org_dir.osprey.gccs.nis. created
ethers.org_dir.osprey.gccs.nis. created
hosts.org_dir.osprey.gccs.nis. created
mail_aliases.org_dir.osprey.gccs.nis. created
sendmailvars.org_dir.osprey.gccs.nis. created
netmasks.org_dir.osprey.gccs.nis. created
netgroup.org_dir.osprey.gccs.nis. created
networks.org_dir.osprey.gccs.nis. created
protocols.org_dir.osprey.gccs.nis. created
rpc.org_dir.osprey.gccs.nis. created
services.org_dir.osprey.gccs.nis. created
timezone.org_dir.osprey.gccs.nis. created

adding credential for osprey.osprey.gccs.nis...
Enter login password:
```

4. Enter the **root password** and press <**Return**>.

```
Wrote secret key into /etc/.rootkey

setting NIS+ group admin.osprey.gccs.nis. ...

restarting root server at security level 2 ...

The system is now configured as a root server for domain
osprey.gccs.nis.
You can now populate the standard NIS+ tables by using the
nispopulate or /usr/lib/nis/nisaddent commands.

NIS+ Domainname         : osprey.gccs.nis.
Directory Path               : /etc/nis

Is this information correct? (Y or N)
```

5. Answer [**y**]and press <**Return**>.

```
This script will populate the following NIS+ tables for domain
osprey.gccs.nis. from the files in /etc/nis:
auto_master auto_home ethers group hosts networks passwd protocols services rpc netmasks bootparams
netgroup aliases shadow

Do you want to continue? (Y or N)
```

6. Answer [**y**] and press <**Return**>.

```
populating auto_master table from file /etc/nis/auto_master...
auto_master table done.

populating auto_home table from file /etc/nis/auto_home...
auto_home table done.

**WARNING: file /etc/nis/ethers does not exist!
        ethers table will not be loaded.

populating group table from file /etc/nis/group...
group table done.

populating hosts table from file /etc/nis/hosts...
hosts table done.

Populating the NIS+ credential table for domain osprey.gccs.nis.
from hosts table.  The passwd used will be nisplus.

dumping hosts table...
loading credential table...

The credential table for domain osprey.gccs.nis. has been populated.

populating networks table from file /etc/nis/networks...
networks table done.

populating passwd table from file /etc/nis/passwd...
passwd table done.

Populating the NIS+ credential table for domain osprey.gccs.nis.
from passwd table.  The passwd used will be nisplus.

dumping passwd table...
loading credential table...

The credential table for domain osprey.gccs.nis. has been populated.

**WARNING: file /etc/nis/protocols does not exist!
        protocols table will not be loaded.
```

```
**WARNING: file /etc/nis/services does not exist!
        services table will not be loaded.

**WARNING: file /etc/nis/rpc does not exist!
        rpc table will not be loaded.

**WARNING: file /etc/nis/netmasks does not exist!
        netmasks table will not be loaded.

**WARNING: file /etc/nis/bootparams does not exist!
        bootparams table will not be loaded.

populating netgroup table from file /etc/nis/netgroup...
netgroup table done.

**WARNING: file /etc/nis/aliases does not exist!
        aliases table will not be loaded.

populating shadow table from file /etc/nis/shadow...
shadow table done.

nispopulate failed to populate the following tables:
ethers protocols services rpc netmasks bootparams aliases
Rebooting the system to activate NIS+, hit return when ready.
```

7. Press <**Return**> when ready to reboot.

8. Login as root and execute the following to complete the installation of the NIS+ server:

   /etc/nis/admin/nis_server_post <**Return**>

```
Added  "secman.osprey.gccs.nis."  to group  "admin.osprey.gccs.nis."

Please enter the network password that your administrator gave you.

Please enter the Secure-RPC password for secman:
```

9. Enter [**nisplus**] and press <**Return**>.

```
Please enter the login password for secman:
```

10. Enter [**vinson**] and press **<Return>**.

11. If this system is sharing file systems the "*/etc/dfs/dfstab*" will have to be modified to use the NIS "netgroup" file to restrict access. To determine if the system is sharing any file systems execute the following:

    `/usr/sbin/share` <**Return**>

```
-          /h/USERS    anon=0    " "
```

12. Line (s) similar to the one shown above should be displayed if the platform is sharing file systems.

13. To restrict access to the "anon=0" file systems script has been provided that modifies the */etc/dfs/dfstab* file. To execute this script do the following:

    `cd /etc/nis/admin` <**Return**>
    `./netgroup_share` <**Return**>

```
Enter the group name you wish to use, name [allowed] recommended.
```

14. The GCCS COE Kernel built the NIS+ "netgroup" file with a group name of "allowed". If you are using that "netgroup" enter "allowed". Otherwise, use the group name you specified and press **<Return>**.

6.3.3 NIS+ Server Checkout

1. The */etc/nsswitch.nisplus* is replaced by the */etc/nsswitch.conf* file used by GCCS. Consequently the correct "nsswitch.conf" file should be in place after the NIS+ server is initialized. The file should look like the following. Note the "automount" and "network" entries are now "nisplus files" vs just "files" in GCCS 2.1.

```
#
# /etc/nsswitch.nisplus:
#
# An example file that could be copied over to /etc/nsswitch.conf; it
# uses NIS+ (NIS Version 3) in conjunction with files.
#
# "hosts:" and "services:" in this file are used only if the
/etc/netconfig
# file contains "switch.so" as a nametoaddr library for "inet"
transports.

# the following two lines obviate the "+" entry in /etc/passwd and
/etc/group.
passwd:      nisplus files
group:       files nisplus

# You must also set up the /etc/resolv.conf file for
# DNS name server lookup.  See resolv.conf(4).
hosts:         files dns nisplus [NOTFOUND=return]

services:      files
# "networks"   added to nisplus for GCCS 2.2
networks:      nisplus files
protocols:     files
rpc:           files
ethers:        files
netmasks:      files
bootparams:    files

publickey:     nisplus

netgroup:      nisplus

# "automount" added to nisplus for GCCS 2.2
automount:     files nisplus
aliases:       files nisplus
sendmailvars:  files nisplus
```

2. Verify that NIS+ is operating correctly by executing the following:

   niscat passwd.org_dir <Return>

```
secman:puNbJU.apVpGc:100:1:Security
Admin:/h/USERS/secman/Scripts:/bin/csh:9654::::::
```

niscat group.org_dir <Return>

NOTE: Only “gccs” and “admin” will appear if AMHS is not used at your site.

```
gccs::100:secman
admin::101:secman
topic::200:amhs_dba
amh_cwp::201:amhs_dba
amh_excl::202:amhs_dba
amh_fbis::203:amhs_dba
amh_limd::204:amhs_dba
amh_nato::205:amhs_dba
amh_pers::206:amhs_dba
amh_spec::207:amhs_dba
amh_ts::208:amhs_dba
amh_rel::209:amhs_dba
```

6.4 Installing Sybase

6.4.1 Required Information

A new Sybase segment has been created that is self initializing, eliminating the need to manually configure and initialize Sybase. You will be required to know the following information before installing Sybase.

a. Will raw disk partitions or UNIX files systems be used: Raw:_____ File Systems:_____
b. Identify Devices:

1. Raw disk partitions (GCCS Standard): c0t2d0s4, c0t2d0s5, etc.

Master Device (17MB): _____
Systemprocs Device (12MB): _____
DB Device (100MB): _____
Log Device (100MB): _____

Or

2. UNIX directory (i.e. /home2/sybase): _____

c. Will Sybase database provided with segment be used to initialize Sybase: Yes: ___ No: ___
d. Location of site provided Sybase backup if used: _____
e. Sybase "sa" password: _____.

6.4.2 Loading Sybase Segment

Load the Sybase 10.0.2 segment using the Segment Installer. The following questions/dialog will appear during the installation.

Table 6.4.2-1. GCCS 2.2 Segment Release Installation

Application	Version	Size	Tape	Comments
Executive Manager Only Segments				
SYBASE	10.0.2.05		2.2 (AP.2)	

Perform the following steps:

```
Identify if you are building the primary or a hot/cold  backup Sybase
server

1) Primary Sybase Server
2) Hot Backup Sybase Server
3) Cold Backup Sybase Server
Sybase Server Type?
```

1. Enter [**1**] and press <**Return**>.

```
You are building a Primary Sybase Server

Is this description correct?(y/n)[n]:
```

2. Enter **[y]** and press <**Return**>.

NOTE: GCCS does not provide licenses for hot backup Sybase servers. The site is responsible for obtaining the appropriate licenses.

```
Are you using raw disk partitions for Sybase?(y/n)[n]:
```

3. Enter the appropriate answer and press <**Return**>. If you are not using raw partitions go to step 12.

```
Enter the 17MB partiton (i.e. c0t2d0s4) used for MASTER Device:
```

4. Enter the correct paritition and press <**Return**>.

```
You have entered:   c0t2d0s4

Is this the correct partition?(y/n)[n]:
```

5. Enter **[y]** and press <**Return**>.

```
Warning: Current Disk has mounted partitions.

==========================================
The partition exist and is the correct size.
==========================================

Enter the 12MB partiton (i.e. c0t2d0s4) used for SYSTEMPROCS Device:
```

6. Enter correct partition and press <**Return**>.

```
You have entered:   c0t2d0s5

Is this the correct partition?(y/n)[n]:
```

7. Enter **[y]** and press <**Return**>.

```
Warning: Current Disk has mounted partitions.

==========================================
The partition exist and is the correct size.
==========================================


Enter the 100MB partiton (i.e. c0t2d0s4) used for DB Device
```

8. Enter the correct partition and press <**Return**>.

```
You have entered:   <example:  c0t2d0s6>

Is this the correct partition?(y/n)[n]:
```

9. Enter **[y]** and press <**Return**>.

```
Warning: Current Disk has mounted partitions.

==========================================
The partition exist and is the correct size.
==========================================


Enter the 100MB partiton (i.e. c0t2d0s4) used for LOG Device:
```

10. Enter the correct partition and press <**Return**>.

```
You have entered:   <example:  c0t2d0s6>

Is this the correct partition?(y/n)[n]:
```

11. Enter **[y]** and press <**Return**>. Go to step 14 to continue.

```
NOTE: The following appears if you are not using raw partitions.

WARNING: The directory you specify must have
at least 229 Mbytes of available disk space.

You must enter the full path along with the directory where
the Sybase database will be stored. (i.e. /home1/sybase)

Enter the directory where the Sybase database will be stored:
```

12. Enter the specified directory and press <**Return**>.

```
NOTE: The following appears if you are not using raw partitions.

You have entered: <example: /home2/sybase >

Is this the correct file system?(y/n)[n]:
```

13. Enter **[y]** and press <**Return**>.

```
You may use the default Sybase dump provided with this segment
or a Sybase dump created at your site (e.g. by System Maintenance)

Do you want to use the default Sybase dump (y/n) [y]:
```

14. Answer [**y**] if you intend to use the Sybse dump provided with the segment or [**n**] if you wish to use a Sybase dump created at your site, then press <**Return**>.

```
Asked if not using default Sybase dump.

Please enter entire path and file name of Sybase dump file
(for example /h/USERS/BACKUP/sybase/db_saves/gccs_dump)
:
```

15. Enter the requested information and press <**Return**>.

```
Asked if not using default Sybase dump.

You have entered /h/USERS/BACKUP/sybase/db_saves/gccs_dump.091296

Is this the correct path(y/n)[n]:
```

16. Answer **[y]** if correct and press <**Return**>.

xterm with title "Setting Partition Permissions "
(Appears only if raw partitions are being used.)

```
crw-------   1 sybase   sys       32, 20 Sep 28 17:14
/dev/rdsk/c0t2d0s4
crw-------   1 sybase   sys       32, 21 Sep 28 17:14
/dev/rdsk/c0t2d0s5
crw-------   1 sybase   sys       32, 22 Sep 28 17:14
/dev/rdsk/c0t2d0s6
crw-------   1 sybase   sys       32, 23 Sep 28 17:14
/dev/rdsk/c0t2d0s7
```

17. Press **<Return>** to clear the widow. Not displayed if using UNIX file systems.

xterm with title “Sybase Initialization”

```
The log file for this session is
'/h/COTS/SYBASE/init/logs/log0929.001'.
Port '6500' is registered to 'u6sybase'.  Either choose a different
port address or make sure that this port is available before
continuing.
Running task to update SQL Server entry in interfaces file.
Task to update SQL Server entry in interfaces file succeeded.
Running task to create the master device.
Building the master device
...............................Done
Task to create the master device succeeded.
Running task to update the SQL Server runserver file.
Task to update the SQL Server runserver file succeeded.
Running task to boot the SQL Server.
waiting for server 'GCCS' to boot...
Task to boot the SQL Server succeeded.
Running task to create the sybsystemprocs database.
sybsystemprocs database created.
Task to create the sybsystemprocs database succeeded.
Running task to install system stored procedures.
.....................................................................
.....................................
...............................Done
Task to install system stored procedures succeeded.
Running task to set permissions for the 'model' database.
.Done
Task to set permissions for the 'model' database succeeded.
Running task to set the default character set and/or default sort
order for the SQL Server.
Setting the default character set to iso_1
Sort order 'binary' has already been installed.
Character set 'iso_1' is already the default.
Sort order 'binary' is already the default.
Task to set the default character set and/or default sort order for
the SQL Server succeeded.
Running task to set the default language.
Setting the default language to us_english
Language 'us_english' is already the default.
Task to set the default language succeeded.
Configuration completed successfully.
Exiting.
The log file for this session is
'/h/COTS/SYBASE/init/logs/log0929.001'.
```

```
Password correctly set.
Account unlocked.
New login created.
(return status = 0)
New user added.
(return status = 0)
```

18. Sybase database is now up and running.

```
xterm titled "Sybase "sa" Password"

Enter new sa password:
sybase1
Password correctly set.
(return status = 0)
```

19. Enter the Sybase "sa" password and press **<Return>**.

6.5 Running "Update_for_Groups" Script

Prior to adding any user accounts the "**update_for_groups**" script located in */h/EM/systools* must be executed. This script converts all the projects and positions into UNIX groups, among other less obvious things. To execute this script do the following:

1. Login as sysadmin and execute the following:

   cd /h/EM/systools <Return>
   ./update_for_groups | tee update_log <Return>

2. Output similiar to the following should be observered or should be seen in the update_log file.

```
Processing Projects...
Created Group = 'Prj_9000', Group Id = '9000'
Added group for Project = 'Day To Day Operations', Group Name =
'Prj_9000', Group Id = '9000'
Created Group = 'Prj_9001', Group Id = '9001'
Added group for Project = 'GCCS', Group Name = 'Prj_9001', Group Id =
'9001'

Processing Positions...
Created Group = 'Pos_9002', Group Id = '9002'
Added group for Project = 'GCCS', Position = 'GCCSUSER', Group Name =
'Pos_9002', Group Id = '9002'
Created Group = 'Pos_9003', Group Id = '9003'
Added group for Project = 'GCCS', Position = 'SYSADMIN', Group Name =
'Pos_9003', Group Id = '9003'
Created Group = 'Pos_9004', Group Id = '9004'
Added group for Project = 'GCCS', Position = 'SYSMAN', Group Name =
'Pos_9004', Group Id = '9004'
Created Group = 'Pos_9005', Group Id = '9005'
Added group for Project = 'Day To Day Operations', Position = 'USER',
Group Name = 'Pos_9005', Group Id = '9005'

Processing User Profiles...
Added User = 'Security Admin' to Group = 'Prj_9001       '.
Added User = 'secman' to Group = 'Pos_9003       '
User = 'sysadmin', already a member of Group = 'Prj_9001       '.
Added User = 'System Manager' to Group = 'Prj_9001       '.
User = 'sysadmin', already a member of Group = 'Pos_9002       '.
Added User = 'sysadmin' to Group = 'Pos_9002       '

Processing Project Files...
Executed: 'chgrp -R  9000 /usr/users/sysadmin/User_Storage
Executed: 'chgrp -R  9001
/usr/edss/global_folder/project/GCCS_30950030

Processing Position Files...
Executed: 'chgrp -R  9002
/usr/edss/global_folder/position/GCCS_30950029/GCCSUSER_30950032
Executed: 'chgrp -R  9003
/usr/edss/global_folder/position/GCCS_30950029/SYSADMIN_30950034
Executed: 'chgrp -R  9004
/usr/edss/global_folder/position/GCCS_30950029/SYSMAN_30950035
Executed: 'chgrp -R  9005
/usr/edss/global_folder/position/dtd40/USER32
```

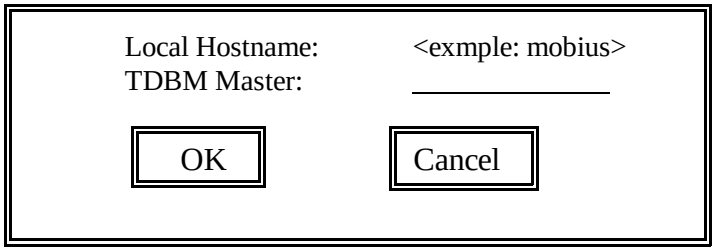
6.6 Loading User Account Groups

Prior to creating any user accounts or loading any applications on the EM server the GCCS COE account group and the Kernel Patch 3 segment must be loaded. In addition if the Character based interface is used the CharIF account group must be loaded. The GCCS COE and CharIF account group segments are located on Application Tape 1; the Kernel Patch 3 segment is located on "hornet" at the OSF. To load these segments execute the following:

1. Bring up the Segment Installer and select the Kernel Patch 3 segment for installation. Do not reboot the system until the GCCS COE is loaded and configured.

2. After the Kernel Patch 3 segment is installed select the latest version of the GCCS COE 2.2 segment for installation. If using tape, insure that you specify */dev/rmt/0mbn*. GCCS COE is actually three segments (GCCS COE, UB Core, and Link 11) and will only load successfully if the "b" option is used.

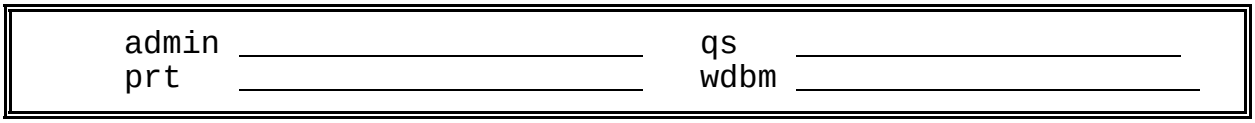
3. After the successful completion of the installation you will be instructed to configure the system by selecting "System Configuration" from the "Networks" menu. This will display the "SysCon Window". If the SysCon GUI looks like the following, you must cancel and restart the system prior to continuing.



4. On the right side of the SysCon Window verify that the hostname in the Local Hostname: field is your workstation's hostname.

5. In the TDBM Master: field, enter the TDBM Server hostname for your workstation. If no TDBM master server exist at your site enter the hostname of the EM server.

6. Any hostname may be entered in the following fields, but typically in the GCCS environment they should all be the TDBM server hostname. If no TDBM master server exist at your site enter the hostname of the EM server.



7. On the left side of the SysCon Window the Full Host #1 will be the hostname of the TDBM Master. You may add additional hosts by clicking on the toggle box beside the host entry you wish to change. When the toggle box is activated (**yellow**), the host is designated as a Full host; and when the toggle box is deactivated (**empty**), it is designated as a Printer host.

NOTE: On GCCS networks, the 5 printer host fields should always be left empty.

---

8. Click the name field next to the appropriate toggle box. The field will become active and is now editable. Enter the name of the host.

9. Click [**OK**] to save the changes you have made to the Hosts box.

10. After the system is configured you should reboot the system as instructed, using the "Restart" option under the "System" menu.

11. If the Character based interface is to be used the CharIF account group should be loaded next. There is no special configuration required when loading this segment.

6.7 Loading Required Segments

Table 6.7-1 list all the segments that must be installed on the Executive Manager server. Any special instructions required when installing the segment are listed in the comments field. All the segments are installed using the Segment Installer.

Table 6.7-1. GCCS 2.2 Core and Network Management Segments

Application	Version	Size	Tape	Comments
GCCS Core Segments				
Applix	3.2	92379	2.2 (AP.1)	Must be loaded before CCAPPS
ASET Client	gv.1.02	25	2.2 (AP.1)	ASETSV Must be installed first
Aset Server	gv.1.04.03	2233	2.2 (AP.2)	
Auditing	3.0.04	112	2.2 (AP.1)	
BSM Patch.P1	1.1.06	20	2.2 (AP.1)	Load patch before deinstalling old audit segments
Cmd Ctr Apps	3.1.2	103166	2.2 (AP.1)	
EM Patch	6.0.1	22462	2.2 (AP.1)	Load only on an upgrade from 2.1to 2.2
EM Printer Admin	2.3.1.04	3084	2.2 (AP.1)	

Table 6.7-1. GCCS 2.2 Core and Network Management Segments (Cont.)

filemgr	1.0	19	2.2 (AP.1)	
GCCS COE	2.2.0.5.02	68153	2.2 (AP.1)	Must reboot after configuring.
GCOEPTC	1.0.02		2.2.2 (AP.1)	
Kernel Patch 3	1.5	370	2.2.1 (UP.1)	Must reboot after loading.
GCCS ftp tool	4.3	342	2.2 (AP.1)	
ICON FOR APPLIX	1.0	21	2.2 (AP.1)	Install if not using Sybase
Mail Services	2.2	2830	2.2 (AP.2)	
PERL	6.0	4720	2.2 (AP.1)	
Remote Install	1.1.1	2068	2.2 (AP.1)	
Run_Remote	1.3.02	86	2.2 (AP.1)	
System Maintenance	2.2	421	2.2.1 (UP.1)	
Tcl/Tk Application	1.0.0	10504	2.2.2 (AP.1)	
Unix Systems MGMT Agent	2.0.0.02	985	2.2 (AP.1)	
UPSI Power Monitor	1.3.b	411	2.2 (AP.1)	Cable must be connected prior to installation. Load only if using UPSI system.
WABI Desktop	2.1	10133	2.2 (AP.2)	
XLOCK ICON	1.0	21	2.2 (AP.1)	
Network Management Segments				
NETM Memory Config	1.0.04	26	2.2 (AP.2)	
Network Monitoring Agent	4.5.03	26820	2.2 (AP.2)	

6.8 Building a Kernel Network Installer

The GCCS COE Kernel Version 2.2 tape contains two tar files. The first tar file is used to load the GCCS COE Kernel directly from tape. The second file can be placed on a shared file system and loaded over the network. This option is significantly faster than using tape. The following steps show how to make the EM server a Kernel Network Installer, although any platform with sufficient disk space can be used.

1. Load the tape in a tape drive and execute the following:

   `cd /h/data/global`

```
mt -f /dev/rmt/0mn fsf 1 <Return>
tar xvf /dev/rmt/0m <Return>
```

2. A file named "kernel_2.2_tar" will be extracted from the tape. This file is approximately 66MB in size. You should insure that "*/h/data/global*" has sufficient disk space to hold this file.

SECTION 7. BUILDING THE GCCS CORE SYSTEM

7.1 Scope

This section addresses the segments that must be installed on all GCCS systems, except EM servers, remote, and standalone systems which are covered in separate sections. It also provides detailed instructions for configuring the core GCCS system. Any SUN software packages should have been loaded (Section 5) prior to executing this section.

7.2 Initializing NIS+ Client

Before loading any segments the system should be initialized as a NIS+ client. This section assumes the NIS+ server (usually the EM server) has been initialized. Execute the following to initialize this NIS+ client.

Login as root and execute the following:

`cd /etc/nis/admin` <**Return**>
`cat nis_client` <**Return**>

```
Following an example of "nis_client" script

/usr/lib/nis/nisclient  -I -d facit.gccs.nis. -h  facit
```

1. Verify that the "nis_client" script has the correct NIS+ domain name following the "-d" (example: facit.gccs.nis.) and the correct NIS+ server name or IP address following the "-h" (example: facit). If they are not correct the script.

2. To initialize this platform as a NIS+ client execute the following:

   `./nis_client` <**Return**>

```
Initializing client <example: hardey> for domain "example:
facit.gccs.nis.>"...
Once initialization is done, you will need to reboot your
machine.

Do you want to continue?  (Y or N)
```

3. Answer [**y**] and press <**Return**>.

```
setting up domain information "<example: facit.gccs.nis. >"...
Can't open /etc/defaultdomain
mv: cannot access /etc/defaultdomain

setting up the name service switch information...

Please enter the network password that your administrator gave you.
Please enter the Secure-RPC password for root:
```

4. Enter "**nisplus"** if the platform is being initialized for the first time as a NIS+ client in this NIS+ domain. Enter the root password if the platform was previously a NIS+ client in this NIS+ domain.

```
Please enter the login password for root:
```

5. Enter the **root password** and press **<Return>**.

```
Client initialization completed!!
Please reboot your machine for changes to take effect.
```

6. Before rebooting execute the following:

   `cat /etc/nsswitch.conf` **<Return>**

```
#
# /etc/nsswitch.nisplus:
#
# An example file that could be copied over to /etc/nsswitch.conf; it
# uses NIS+ (NIS Version 3) in conjunction with files.
#
# "hosts:" and "services:" in this file are used only if the
/etc/netconfig
# file contains "switch.so" as a name to addr library for "inet"
transports.

# the following two lines obviate the "+" entry in /etc/passwd and
/etc/group.
passwd:       nisplus files
group:        files nisplus

# You must also set up the /etc/resolv.conf file for
# DNS name server lookup.  See resolv.conf(4).
hosts:          files dns nisplus [NOTFOUND=return]

services:     files
# "networks" added to nisplus for GCCS 2.2
networks:     nisplus files
protocols:    files
rpc:          files
ethers:       files
netmasks:     files
bootparams:   files

publickey:    nisplus

netgroup:     nisplus

# "automount" added to nisplus for GCCS 2.2
automount:    files nisplus
aliases:      files nisplus
sendmailvars: files nisplus
```

7. The */etc/nsswitch.nisplus* is replaced by the */etc/nsswitch.conf* file used by GCCS. Consequently the correct "nsswitch.conf" file should be in place after the NIS+ server is initialized. The file should look like the following. Note the "automount" and "network" entries are now "nisplus files" vs just "files" in GCCS 2.1.

8. If this system is sharing file systems the "*/etc/dfs/dfstab*" will have to be modified to use the NIS "netgroup" file to restrict access. To determine if the system is sharing any file systems execute the following:

`/usr/sbin/share` <**Return**>

```
    -/h/USERS    anon=0    " "
```

9. Line(s) similar the one shown above should be displayed if the platform is sharing file systems.

10. To restrict access to the "anon=0" file systems a script has been provided that modifies the */etc/dfs/dfstab* file. To execute this script do the following:

    `cd /etc/nis/admin` <**Return**>
    `./netgroup_share` <**Return**>

```
Enter the group name you wish to use, name [allowed] recommended"
```

11. The GCCS COE Kernel built the NIS+ "netgroup" file with a group name of "allowed". If you are using that "netgroup" enter "allowed". Otherwise, use the group name you specified and press <**Return**>.

12. If the */etc/nsswitch.conf* file is correct reboot the system by executing the following.

    `uadmin 2 1` <**Return**>

13. Verify that NIS+ is operating correctly by executing the following:

    `niscat passwd.org_dir` <**Return**>

```
secman:puNbJU.apVpGc:100:1:Security
Admin:/h/USERS/secman/Scripts:/bin/csh:9654::::::
```

14. At a minimum the line shown above should be in the NIS+ password database.

7.3 Post GCCS COE Kernel Installation Procedures

Prior to loading any applications the GCCS COE segment must be installed and configured. In addition the Kernel Patch 3 segment must be installed to update several functions in the system. If the Character based accounts are being used, the CharIF account group must be loaded. All of these segments are available on Application Tape 1, except for Kernel Patch 3, which is available on "hornet" at the OSF. Execute the

following:

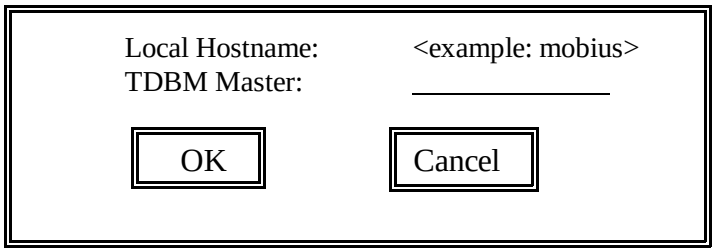
1. Bring up the Segment Installer and select the Kernel Patch 3 segment for installation. Do not reboot the system until the GCCS COE is loaded and configured.

NOTE: Disregard warning message displayed during Kernel Patch 3 installation.

---

2. After the Kernel Patch 3 is installed select the latest version of the GCCS COE 2.2 segment for installation. If using tape, insure that you specify */dev/rmt/0mbn*. GCCS COE is actually three segments (GCCS COE, UB Core, and Link 11) and will only load successfully if the "*b*" option is used.

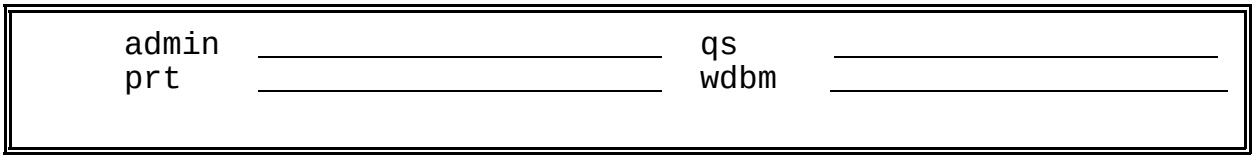
3. After the successful completion of the installation you will be instructed to configure the system by selecting "System Configuration" from the "Networks" menu. This will display the SysCon GUI. If the SysCon GUI looks like the following, you must cancel and restart the system prior to continuing.



4. On the right side of the SysCon Window verify that the hostname in the Local Hostname: field is your workstation's hostname.

5. In the TDBM Master: field, enter the TDBM Server hostname for your workstation. If no TDBM master server exist at your site enter the hostname of the EM server.

6. Any hostname may be entered in the following fields, but typically in the GCCS environment they should all be the TDBM server hostname. If no TDBM master server exist at your site enter the hostname of the EM server.



7. On the left side of the SysCon Window the Full Host #1 will be the hostname of the TDBM Master. You may add additional hosts by clicking on the toggle box beside the host entry you wish to change. When the toggle box is activated (**yellow**), the host is designated as a Full host; and when the toggle box is deactivated (**empty**), it is designated as a Printer host.

NOTE: On GCCS networks, the 5 printer host fields should always be left empty.

---

8. Click the name field next to the appropriate toggle box. The field will become active and is now editable. Enter the name of the host.

9. Click OK to save the changes you have made to the Hosts box.

10. After the system is configured you should reboot the system as instructed, using the "Restart" option under the "System" menu.

11. If the Character based interface is to be used the CharIF account group should be loaded next. There is no special configuration required when loading this segment.

7.4 Loading Required Segments

Table 7.4-1 list all the Core and Network Management Segments that should be loaded on each GCCS system. Any special instructions required when installing the segments are listed in the comments field. All the segments are installed using the Segment Installer.

Table 7.4-1. GCCS 2.2 Core and Network Management Segments

Application	Version	Size	Tape	Comments
GCCS Core Segments				
Applix	3.2	92379	2.2 (AP.1)	Must be loaded before CCAPPS
ASET Client	gv.1.02	25	2.2 (AP.1)	ASETSV Must be installed first
Aset Server	gv.1.04.03	2233	2.2 (AP.2)	
Auditing	3.0.04	112	2.2 (AP.1)	
BSM Patch.P1	1.1.06	20	2.2 (AP.1)	Load patch before deinstalling old audit segments
Cmd Ctr Apps	3.1.2	103166	2.2 (AP.1)	
EM Patch	6.0.1	22462	2.2 (AP.1)	Load only on an upgrade from 2.1to 2.2
EM Printer Admin	2.3.1.04	3084	2.2 (AP.1)	

Table 7.4-1. GCCS 2.2 Core and Network Management Segments (Cont.)

filemgr	1.0	19	2.2 (AP.1)	
GCCS COE	2.2.0.5.02	68153	2.2 (AP.1)	Must reboot after configuring.
GCOEPTC	1.0.02		2.2.2 (AP.1)	
Kernel Patch 3	1.5	370	2.2.1 (UP.1)	Must reboot after loading.
GCCS ftp tool	4.3	342	2.2 (AP.1)	
ICON FOR APPLIX	1.0	21	2.2 (AP.1)	Install if not using Sybase
Mail Services	2.2	2830	2.2 (AP.2)	
PERL	6.0	4720	2.2 (AP.1)	
Remote Install	1.1.1	2068	2.2 (AP.1)	
Run_Remote	1.3.02	86	2.2 (AP.1)	
System Maintenance	2.2	421	2.2.1 (UP.1)	
Tcl/Tk Application	1.0.0	10504	2.2 (AP.1)	
Unix Systems MGMT Agent	2.0.0.02	985	2.2 (AP.1)	
UPSI Power Monitor	1.3.b	411	2.2 (AP.1)	Cable must be connected prior to installation. Load only if using UPSI system.
WABI Desktop	2.1	10133	2.2 (AP.2)	
XLOCK ICON	1.0	21	2.2 (AP.1)	
Network Management Segments				
NETM Memory Config	1.0.04	26	2.2 (AP.2)	
Network Monitoring Agent	4.5.03	26820	2.2 (AP.2)	

7.5 Configuring Auditing

The latest version of the Auditing segment automatically configures the system to do auditing. After loading the segment you will be instructed to boot the system in single user mode and run the "bsmconv" command.

Perform the following steps:

1. After loading the Auditing segment exit the Segment Installer and execute the following to initialize

auditing:

`uadmin 2 0` <**Return**>
`ok  boot -s` <**Return**>

```
INIT:      SINGLE USER MODE

type Ctrl-d to proceed with normal startup
(or give root password for system maintenance):
```

2. Enter the "**root**" password and press <**Return**>.

3. Enter the following to initialize auditing:

   `cd /etc/security` <**Return**>
   `bsmconv` <**Return**>

4. Reboot the system by executing the following:

   `uadmin 2 1` <**Return**>

7.6 Configuring Printing

After loading the *Printer Administration* segment you will define your printers if they have not been previously defined. Each user will also be required to select which printers they wish to have available.

7.7 Where To Next

The sections listed below provide instructions on loading the various categories of applications available in GCCS. You may be installing applications from all these sections, except for Section 10, which is for Oracle Database Servers only. Go to the appropriate sections to continue the installation process. Note, if you are performing an upgrade on the Oracle Database Server, you should go to section 10.2. Section 10.3 is only for building Oracle Database Servers from the operating system up.

Section 8	Building JOPES Application Server.
Section 9	Building JOPES SPARC Client.
Section 10	Building Oracle Database Server.
Section 11	Building A Unified Build SUN Platform.
Section 12	Teleconferencing Installation Procedures.
Section 13	Building Character Based Server.
Section 15	Loading GCCS Mission Applications.

SECTION 8. BUILDING JOPES APPLICATION SERVER

The standard GCCS Application Server is a SPARC 20 with 224 Mbytes of RAM and approximately 4GBytes of disk space. A JOPES Application server should have all the JOPES applications, which are required by a site, installed on it. In addition the Teleconferencing segments must be installed.

Table 8-1 list all the JOPES application segments, the Teleconferencing segments, and the supportting segments that should be loaded on a JOPES application server. The segments are listed in alphabetic order versus order of installation. The segments listed below should be loaded first, in the order shown. This will address the requirements of all the remaining applications.

- Netscape
- JOPES Navigation
- ORACLE Apps Server Tools
- External Transaction Processor
- Requirements Development and Analysis

Table 8-1. GCCS JOPES Application and Teleconferencing Segments

Application	Version	Size	Tape	Comments
JOPES Application Segments				
AdHoc Query Graphic	5.6.0.2.03		2.2 (AP.1)	
DART Client	3.1		2.2 (AP.1)	
External Transaction Processor	5.6.0.8		2.2.1 (UP.1)	
GSORTS MAP/RETRIEVAL	2.0		2.2 (AP.1)	Known as : 'map/retrieval'
Patch 1 for GSORTS 2.0	2.1		2.2.1 (UP.1)	
GSORTS.P2	2.3		2.2.2 (UP.1)	
IMS-RFM Client	2.0.8	37	2.2 (AP.1)	Load IMS-RFM on Oracle database server
JEPES Client	4.04.0.02		2.2 (AP.1)	
JOPES Navigation	2.7.0.02		2.2 (AP.1)	
JOPES_PDRPT v2.2.1 Clt	2.2.1		2.2 (AP.1)	
LOGSAFE Client	2.8.0.02		2.2 (AP.1)	
Medical Planning and Execution System	5.5.401f		2.2 (AP.1)	
NPG	5.5.3b		2.2 (AP.1)	

Oracle Application Server Tools	7.1.4.06		2.2 (AP.1)	
Predefined Reports	1.6.2.01		2.2 (AP.1)	
Requirements Development and Analysis (RDA)	1.8.2.01		2.2.1 (UP.1)	
S&M Graphic	5.6.0.0.02		2.2 (AP.1)	
TCC Extrnl Sys Intrfcs	1.2.2		2.2 (AP.1)	
Teleconferencing Segments				
Internet Relay Chat Clients	1.1	6716	2.2 (AP.1)	
IRC Client Patch 1	1.0	22	2.2 (AP.1)	
Netscape Web Browser	3.0.02		2.2.1 (UP.1)	

SECTION 9. BUILDING JOPES SPARC CLIENT

The standard GCCS JOPES SPARC client is a SPARC with 64 Mbytes of RAM and approximately 2GBytes of disk space. The limited amount of memory limits the number of applications that may be run simultaneously. The limited amount of disk space demands that the users select carefully which applications they wish loaded on the system. The majority of the JOPES applications will fit on the standard GCCS JOPES SPARC client with 2Gbytes of disk space.

Table 9-1 list all the JOPES application segments, the Teleconferencing segments, and the supportting segments that may be loaded on a JOPES application server. The segments are listed in alphabetic order versus order of installation. The segments listed below should be loaded first, in the order shown. This will address the requirements of all the remaining applications as well as the limited disk space requirements.

- Netscape
- JOPES Navigation
- ORACLE Apps Server Tools (or ORACLE NFS Application Server Tools)
- External Transaction Processor
- S&M (If it is to be loaded)
- Requirements Development and Analysis

The ORACLE NFS Application Server Tools segment should only be loaded if there is absolutely no disk space availabe for the ORACLE Apps Server Tools (170Mbytes) segment.

Table 9-1. GCCS JOPES Application and Teleconferencing Segments

Application	Version	Size	Tape	Comments
JOPES Application Segments				
AdHoc Query Client	5.4.3	25	2.2 (AP.1)	
AdHoc Query Graphic	5.6.0.2.03		2.2 (AP.1)	
DART Client	3.1		2.2 (AP.1)	
External Transaction Processor	5.6.0.8		2.2.1 (UP.1)	
GSORTS Client	2.0.02		2.2 (AP.1)	
GSORTS MAP/RETRIEVAL	2.0		2.2 (AP.1)	Known as : 'map/retrieval'
Patch 1 for GSORTS 2.0	2.1		2.2.1 (UP.1)	
GSORTS.P2	2.3		2.2.2 (UP.1)	
IMS-RFM Client	2.0.8	37	2.2 (AP.1)	Load IMS-RFM on Oracle database server

Table 9-1. GCCS JOPES Application and Teleconferencing Segments (Cont.)

JEPES Client	4.04.0.02		2.2 (AP.1)	
JOPES Navigation	2.7.0.02		2.2 (AP.1)	
JOPES_PDRPT v2.2.1 Clt	2.2.1		2.2 (AP.1)	
LOGSAFE Client	2.8.0.02		2.2 (AP.1)	
Medical Planning and Execution System	5.5.401f		2.2 (AP.1)	
NPG	5.5.3b		2.2 (AP.1)	
Oracle Application Server Tools	7.1.4.06		2.2 (AP.1)	
Oracle NFS Application Server Tools	1.1		2.2 (AP.1)	Install only if unable to install Oracle tools
PDR	1.6.2.01		2.2 (AP.1)	
Requirements Development and Analysis (RDA)	1.8.2.01		2.2.1 (AP.1)	
S&M Client	5.4.2	35	2.2 (AP.1)	Load only if no disk space available to load S&M Graphic
S&M Graphic	5.6.0.0.02		2.2 (AP.1)	
System Services Client	5.4.2	35	2.2 (AP.1)	Load only if System functionality is required
TCC Extrnl Sys Intrfcs	1.2.2		2.2 (AP.1)	
Teleconferencing Segments				
Internet Relay Chat Clients	1.1	6716	2.2 (AP.1)	
IRC Client Patch 1	1.0	22	2.2 (AP.1)	
Netscape Web Browser	3.0.02		2.2.1 (UP.1)	

SECTION 10. BUILDING ORACLE DATABASE SERVER

10.1 Overview

All the JOPES Oracle Database Servers are in operation and should be upgraded using the procedures outlined in Section 16. Section 10.2 addresses the database upgrades that must be done on the JOPES Oracle Database Servers after the Kernel upgrade has been performed. Section 10.3 addresses the situation where the JOPES Oracle Database Server must be built from the Solaris 2.3 operating system up.

10.2 JOPES Oracle Database Server Upgrade

Table 10-2-1 list all the segments that must be loaded on the JOPES Oracle Database Server to complete the GCCS 2.2 upgrade. The segments are listed in alphabetic order versus order of installation. Key points regarding the order of installation are listed:

- ORACLE Application Server Tools 7.1.4.06 must be loaded first.
- ORACLE RDBMS Patch 2 should be loaded before any other application database segments or patches.
- SMDB Database Patch 15 requires that you have the password for the "SNAPSHOT_MASTER_READER" oracle account on the NMCC Oracle Database server prior to installation. This patch must be installed before RDA Server Patch 13.
- SMDB DB Patch 16 must be loaded before RDA Server Patch 13.

Table 10.2-1. GCCS ORACLE Database Server Update

Application	Version	Size	Tape	Comments
JOPES Application Segments				
External Transaction Processor	5.6.0.8		2.2.1 (UP.1)	
IMS_RFM	5.6.0.0.03		2.2 (DB.1)	
Oracle Application Server Tools	7.1.4.06		2.2 (AP.1)	
JOPES Oracle Database Site Segments				
ESI Server Patch 2	1.2.2.01		2.2 (DB.1)	
GSORTS Oracle Engine (GUPD)	3.2.01		2.2.2 (UP.1)	
GSORTS Oracle Server (GUPD.P1)	3.3		2.2.2 (UP.1)	
GSORTS Oracle Server (GORA.P1)	3.2		2.2.2 (UP.1)	
JEPES Server Patch 4	4.04.0		2.2 (DB.1)	

Table 10-2-1. GCCS ORACLE Database Server Update 2.1 (Cont.)

Logsafe Server Patch 7	2.8.0.02		2.2 (DB.1)	
Predefined Rpts DB Srvr	1.6.2.01		2.2 (DB.1)	
RDA Server Patch 14	1.8.2.02		2.2.1 (UP.1)	
SM	5.6.0.0.02		2.2 (AP.1)	
SM.P1	5.6.0.8.01		2.2.1 (UP.1)	
SM.P2	5.6.0.9		2.2.1 (UP.1)	
S&M Data Base Patch 15	5.5.6.04b		2.2 (DB.1)	
S&M Data Base Patch Segment 16	5.6.0.0.05		2.2 (DB.1)	
Non-JOPES Oracle Database Segments				
Air Field DB Server	2.0	3569	2.2 (DB.1)	
Airfields DB Patch 1	1.0.1.01		2.2.1 (UP.1)	
Oracle Database Server Segments				
Database User	6.0.2		2.2 (DB.1)	
RDBMS Patch 3	3.0.0		2.2.1 (UP.1)	

The ORACLE Apps Server Tools listed in Table 10-2 may be loaded if you wish to recover approximately 284 Mbytes of disk space.

10.3 JOPES Oracle Database Server Build

CAUTION: DO NOT EXECUTE THIS SECTION IF YOU ARE UPGRADING AN ORACLE DATABASE SERVER!

Table 10-3-1 list all the segments that must be loaded on a JOPES Oracle Database Server that is being built after the Solaris 2.3 operating system and GCCS 2.2 Kernel have been installed. The segments are listed in alphabetic order versus order of installation. The following segments should be loaded first in the order shown:

- ORACLE Memory Config
- ORACLE Apps Server Tools
- ORACLE RDBMS
- GSORTS Oracle Server
- S&M Oracle Data Base Segment
- S&M Database Patch 15

C S&M DB Patch 16

Table 10.3-1 GCCS ORACLE Database Server New Build

Application	Version	Size	Tape	Comments
JOPES Application Segments				
DART	2.0.03		2.2 (DB.2)	
External Transaction Processor	5.6.0.8		2.2.1 (UP.1)	
GSORTS WORLD DATA	2.0		2.2 (DB.2)	
IMS_RFM	5.6.0.0.03		2.2 (DB.2)	
Oracle Application Server Tools	7.1.4.06		2.2 (AP.1)	
JOPES Oracle Database Site Segments				
ESI Flat File Allocate	1.2.2.02		2.2 (DB.2)	
GSORTS Oracle Sever (GORA)	3..0.1		2.2.1 (UP.1)	
GSORTS Oracle Server (GUPD)	3.2.01		2.2.2 (UP.1)	
GSORTS Oracle Server (GUPD.P1)	3.3		2.2.2 (UP.1)	
GSORTS Oracle Server (GORA.P1)	3.2		2.2.2 (UP.1)	
JEPES Oracle Server	4.01	21	2.2 (DB.2)	
JOPES_ORA_PDRPT Srv v2.2.1	2.2.1		2.2 (DB.2)	
LOGSAFE DB Server	2.8.0.01		2.2 (DB.2)	
MEPES Oracle data base segment	5.5.402f	34	2.2 (DB.2)	
NPGDB	5.5.5		2.2 (DB.2)	
Predefined Rpts DB Srvr	1.6.2.01		2.2 (DB.2)	
RDA Server	1.8.1		2.2 (DB.2)	
RDA Server Patch 14	1.8.2.02		2.2.1 (UP.1)	
SM	5.6.0.0.02		2.2 (AP.1)	
SM.P1	5.6.0.8.01		2.2.1 (UP.1)	

Table 10.3-1 GCCS ORACLE Database Server New Build (Cont.)

SM.P2	5.6.0.9		2.2.1 (UP.1)	
S&M Data Base Patch 15	5.5.6.04b		2.2 (DB.2)	
S&M Data Base Patch Segment 16	5.6.0.0.05		2.2 (DB.2)	
S&M Oracle data base segment	5.6.0.0		2.2 (DB.2)	
Non-JOPES Oracle Database Segments				
Air Field DB Server	2.0	3569	2.2 (DB.2)	
Airfields DB Patch 1	1.0.1.01		2.2.1 (UP.1)	
Oracle Database Server Segments				
Database User	6.0.2		2.2 (DB.2)	
ORACLE Memory Config	7.1.4.01		2.2 (DB.2)	
ORACLE RDBMS	7.1.4.01		2.2 (DB.2)	Load only if building Oracle Database server from scratch.
ORACLE RDBMS Patch 3	3.0.0		2.2.1 (UP.1)	

SECTION 11. BUILDING A UNIFIED BUILD SUN PLATFORM

11.1 Saving Configuration Information from UB 2.1.3.5

Several configuration items need to be saved and/or taken note of when performing an upgrade of the Unified Build software from 2.1.3.5 to 3.0.1.6G. The following paragraphs outline steps necessary to retain configuration information.

1. Broadcasts: In order to retain the Broadcast configuration for re-entry after the installation of UB3.0.1.6G, perform the following on the TDBM Master machine:

   a. Under the FOTC/Bcst Pull Down Menu (PDM), select Broadcasts.

   b. Highlight a broadcast and select Edit. Print the Edit Window.

   c. Select Header and print the Header Edit Window. Go back tothe previous window and select Filter and print the Filter Edit window.

   d. Repeat for each broadcast. Keep the printouts together for each broadcast.

2. Communications Configuration: In order to retain the Broadcast configuration for rentry after the installation of UB3.0.1.6G, perform the following on the TDBM Master machine:

   a. Under the Comms PDM, select Communications.

   b. Print the list of communications channels.

   c. Double click each communication channel and print each Edit Channel Window.

3. AutoForward Tables: In order to retain the AutoForward table configuration for rentry after the installation of UB3.0.1.6G, perform the following on the TDBM Master machine:

   a. Select AutoForward under the Comms PDM.

   b. Double click each entry and print each Edit Window.

4. DDN Host Table: The DDN Host table can be archived to tape prior to performing the upgrade. Performthe flowing on the TDBM Master machine:

   a. Using the the tar command, save the following two files to tape:

      cd /h/Nauticus/data/mnt; tar cvf <*no rewind tape device*> **Messages/Host-Table Messages/Host-Table-Altr**

5. Overlays, PIMTracks, Screen Kilos, and Four Whiskey Grids: If it is necessary to save the above data it will be necessary to transmit each of the Overlays, PIMTracks, Screen Kilos, and Four Whiskey Grids from the TDBM Master Machine to a different TDBM Master Machine. A site can rename the Overlays, PIMTracks, Screen Kilos, and Four Whiskey Grids to names that are in series (i.e: 001, 002, 003), transmit them to a different TDBM Master Machine, perform the upgrade to UB 3.0.1.6G, and transmit the items back. Sites can convert a TDBM Client on the suite into a TDMB Master or they can coordinate with another site (or the OSF) and transmit the Overlays, PIMTracks, Screen Kilos, and Four Whiskey Grids to that site. When the upgrade is complete, the Overlays, PIMTracks, Screen Kilos, and Four Whiskey Grids can be transmitted back. The procedures for configuring a TDBM Master are in the UB System Administrator Guide. The procedures for transmitting Overlays, PIMTracks, Screen Kilos, and Four Whiskey Grids are documented in the UB Users Guide.

6. Briefs and Stored Slides: Briefs and Stored Slides can be archived to tape and restored after the upgrade to UB 3.0.1.6G is complete.

   a. On the TDBM Master Machine tar the following directory to tape:

      cd /h/Nauticus/data/mnt; tar cvf <*no rewind tape device*> **StoredScreens**

11.2 Loading and Configuring the Required Segments

Install the following application segments in accordance with the steps in this chapter:

- GCCS COE
- JMTK
- UBApps
- JMCISApps
- PRINTER
- Any additional Unified Build GCCS Application Segments (such as Theater Ballistic Missile Defense (TBMD) or ELVIS).

See Table 11-2-1.

Table 11.2-1. GCCS JMCIS Segments

Application	Version	Size	Tape	Comments
JMCIS Segments				
COP Sync Tool	1.0.1.1.01		2.2.2 (AP.2)	
ELVIS	1.4.0.1		2.2.2 (AP.2)	
JMCIS Applications	3.0.1.6.02G		2.2 (AP.1)	

Table 11.2-1. GCCS JMCIS Segments (Cont.)

Joint Mapping Toolkit	3.0.1.6.02G		2.2 (AP.1)	
Link 11/TadilA	3.0.0.0		2.2.2 (UP.1)	
Printer	3.0.1.6.02G		2.2 (AP.1)	
Tactical Information Broadcast System	2.1.4.04		2.2.1 (UP.1)	
TBMD Shared Early Warning	1.0.0.0.01		2.2.1 (UP.1)	
TBMD	3.0.5.5		2.2.2 (UP.1)	
UB Applications	3.0.1.6.02G		2.2 (AP.1)	
UBPATCH	3.0.1.6GP2		2.2 (AP.1)	
UB 3.0.1.6G Patch 5	3.0.1.6GP5		2.2.2 (UP.1)	
UB Suppress	1.0.01		2.2.1 (UP.1)	

For more information regarding segment installation and the **Segment Installer** window, refer to the *Unified Build System Administrator's Guide*.

Login as **sysadmin** (using the default password) and select **SEGMENT INSTALLER** from the Software menu.Airfields DB Patch 1

1. If the tape has not been previously inserted into the tape drive, insert the GCCS Application tape into the tape drive.

2. Install the GCCS COE.

When the GCCS COE segment install is complete, a warning window appears, stating that you must configure the Host/Server settings and reboot the system when the installation is complete.

3. Click OK in the warning window to dismiss it.

4. To configure the Unified Build software, a machine should be designated as the Track Database Master (TDBM). When configuring the software, the TDBM master should appear as the "***_host**" in the SysCon window and should also appear as the first entry in the "**host list**". Configure the TDBM Host and Client(s) settings as follows: (For more details on the SysCon window, see the *Unified Build System Administrator's Guide*.)

    a. From the Network menu, select **System Configuration**. The **SysCon** window appears.

b. To set the hosts, in the Hosts box (on the left side of the window), click the toggle box beside the host entry you wish to change (starting with **Full Host #2**).

c. Click the **Full Host #2** field next to the appropriate toggle box. The field becomes active and is now editable. Enter the name of the host.

NOTE: When entering hostnames, you should enter the name of the local host (*Athis@* machine*'*s hostname) in the Full Host #2 field and any other hosts on the local network (other machines on your local LAN) into the subsequent Full Host fields.

---

d. Verify that the hostname in the Local Hostname: field is your workstation's hostname.

e. In the TDBM Master: field, enter the TDBM Server hostname for your workstation.

f. In the GCCS environment, both the TDBM server and TDBM clients should have the TDBM **server** hostname in each of the following:

admin	***qs***
prt	***wdbm***

NOTE: Typically, in the GCCS environment, both the TDBM server and TDBM clients should have the TDBM server hostname in each of the above fields in the SysCon window. However, to account for diverse configuration capabilities, any hostname may be entered in these fields.

---

g. Click OK to save the changes you have made.

5. Update the local hosts file to reflect the local hosts which will be allowed to communicate with your system (trusted hosts) by using the Edit Local Hosts window. For more details on editing the Local Hosts, see the *Unified Build System Administrator's Guide*.

a. From the Network menu, choose Edit Local Hosts. The EDIT HOSTS window appears.

b. For each of the machines which are to be designated as trusted hosts on your LAN, highlight the IP address which corresponds to the host and click EDIT. The EDIT MACHINE window appears.

NOTE: If a host's IP address does not appear in the list in the EDIT HOSTS window, you may add it by clicking ADD. An ADD MACHINE window, similar to the EDIT MACHINE window, appears.

c. In the EDIT MACHINE window, verify the information in the MACHINE NAME: and MACHINE ADDRESS: fields is correct. If the information in these two fields is not correct, edit it by entering the correct information in the NEW MACHINE NAME: and NEW MACHINE ADDRESS: fields.
d. In the EDIT MACHINE window, click the Trusted Machine checkbox so it is filled (**on**). This host is now a trusted host for the local machine.

e. In the EDIT MACHINE window, click ALIASES. The ALIASES window appears.

f. In the ALIASES window, click **ADD**. The ADD ALIASES window appears.

g. Enter the alias you wish to assign to the host and press [Return] to accept the entry.

IMPORTANT: You must press the [Return] key on your keyboard to accept the entered alias. If you click Cancel in the ALIASES window, the alias information will not be saved.

h. Click **OK** in the Aliases window. The ALIASES window closes, returning you to the EDIT MACHINE window.

i. Click **OK** in the EDIT MACHINE window. The EDIT MACHINE window closes, returning you to the EDIT HOSTS window.

j. Click **OK** in the EDIT HOSTS window.

7. When the GCCS COE install and Host/Server configuration is complete, use the System Reboot option under the Hardware menu to reboot the system.

WARNING: You *must* reboot the workstation after the GCCS COE segment is installed. *Do not load any additional segments without rebooting the workstation*.

8. These segments should be installed in the following order:

- JMTK
- UBApps
- JMCISApps
- PRINTER

9. When the segment installation is complete, a warning window appears stating Selected Segment(s) Installed Successfully.

10. Click the **EXIT** button to dismiss this warning window.

11. Load any additional Unified Build GCCS application segments at this time, using the Segment Installer window.

NOTE: If you wish to do any Elint processing, you must ensure that the machine whose disk serves the /h/data/global/UB directory is loaded with the GCCSSD, Version 2.2.1 segment available on the optional Secret Data tape. Typically, the machine whose disk serves the directory is the EM Server.

---

12. On the Segment Installer window, click **EXIT** to dismiss the window.

13. Using the Logout option under the Hardware menu, log out of the system.

11.3 Restoring Configuration Information from UB 2.1.3.

It is at this point that the information saved prior to upgrade is applied to the UB 3.0.1.6G build. The following paragraphs outline steps necessary to restore configuration information.

1. DDN Host Table: The DDN Host table can be restored from tape after performing the upgrade. After UB 3.0.1.6G has been loaded, un-tar the files as follows:

   cd /h/data/global/UB; tar xvf *<no rewind tape device>* *****

   After the tape has been loaded, log in as sysadmin. From the Network PDM, select Config DDN Host Table and verify that it is correct.

2. Communications Configuration: The Broadcast configuration must be re-entered after the installation of UB 3.0.1.6G. Use the printouts to re-enter the Communications configuration on the TDBM Master machine.

NOTE: It is suggested that sites replace their NETWORK Channel with a new channel that uses the NETPREC Channel.

---

   a. As sysadmin, from the Network PDM, select Set WAN UID and enter the assigned 3 character trigram.

b. As a user, from the Comms PDM, select Communications. Click on the ADD window button. Enter the NAME and the XREF (the XREF need only be locally unique). Select the interface type and the initial settings from the supplied lists of options. Press the -OK- window button. Back at the Communications window, highlight the new entry and press the EDIT window button. Using the printouts created earlier, set the parameters of the communications channel to the proper values and press the OK window button. After the channels have been entered, select Communications under the Comms PDM, hold down the right mouse button (RMB) and select Set Default to store the configuration.

3. Broadcasts: The Broadcast configuration must be re-entered after the installation of UB 3.0.1.6G. Use the printouts to re-enter the Broadcast configuration on the TDBM Master machine. As a user, with the chart up (if not, from the system PDM, select Chart, then Restart Chart), from the chart menubar, select FOTC/Bcst and then Broadcasts. Use the ADD window button to add the new broadcast and the EDIT window button to adjust it.

4. AutoForward Tables: The AutoForward table configuration must be re-entered after the installation of UB 3.0.1.6G. Use the printouts to re-enter the AutoForward configuration on the TDBM Master machine. As a user, from the system menubar, select Comms and then Auto-Forward Table. Use the ADD window button to add each entry back in.

5. Overlays, PIMTracks, Screen Kilos, and Four Whiskey Grids: It is now that the remote site transmits your Overlays, PIMTracks, Screen Kilos, and Four Whiskey Grids back to you. The procedures for transmitting Overlays, PIMTracks, Screen Kilos, and Four Whiskey Grids are documented in the UB Users Guide.

6. Briefs and Stored Slides: Briefs and Stored Slides can be restored from after the upgrade to UB 3.0.1.6G is complete. On the TDBM Master Machine, un-tar the file as follows:

   cd /h/data/global/UB; **tar xvf** <*no rewind tape device*> *****

11.4 Loading Unified Build Maps

The Unified Build software with the Joint Mapping Tool Kit is capable of displaying many DMA mapping products. These include but are not limited to: ARC Digitized Raster Graphics (ADRG), Compressed ADRG (CADRG), Compressed Imagery Base (CIB), and Vector Product Format (VPF) Maps. For details in loading these maps refer to the Unified Build 3.0.1.6G User's Guide.

SECTION 14. BUILDING REMOTE PLATFORMS

14.1 Scope

This section of the Implementation Procedures provides installation instructions for loading, configuring and using remote access SUN SPARC platforms. These segments are used to enable a remote site to connect to a server at host site, via a low-speed STU_III connection. Sun workstations can be configured as "standalone" or "EM_client" workstations.

Standalone systems. These are self-contained workstations, not requiring an EM server, DB server or Sybase. The telecommunications link (e.g., PPP) is only established when access to a remote Applications server is required - typically to run applications with the ASCII interface. This configuration is much more efficient in terms of telecommunications link utilization - more GCCS components are hosted on the 'local' sun workstation, requiring less use of the 'host' system. The standalone configuration is the recommended configuration for remote Sun workstations. However, the desktop folder system is not available since Sybase is not used in this cofiguration. This prevents you from using AMHS and Command Center Apps.

EM_client systems. This configuration acts just like any GCCS client. The telecommunications link is established at system boot time, and remains continuously connected until the workstation is shutdown. While booted, the telecommunications link between the remote client and the host system/site acts like an Ethernet LAN connection, only slower. The disadvantage is that this configuration does not take advantage of the capability of a Sun workstation to host other components of GCCS, but instead uses its network access, which can be very slow, for all GCCS functions. Use of this configuration for remote Sun workstation is not recommended - use a standalone configuration with auto-mounted home directories.

14.2 Information Required to Build a Remote Workstation

14.2.1 Related documentation

Secret IP Router network (SIPRNET) communications Server STU-III operations and Maintenance Guidebook, 28 June 1995, DISA.

NOTE: Prior to installation of software, ensure that the Sun workstation is a Sun SPARC 5 or better, with at least 64 MB RAM and at least 2.1 Gb disk storage.

14.2.2 Question Worksheet

1. Standalone _____.
   or
2. EM Client _____.
3. Cisco 2511 Ethernet Port address _____.
4. Character base Application Server IP address _____.
5. Cisco 2511 asynchronous port IP address _____.

6. Serial Port (a or b) _____.
7. Phone number of communications server _____.
8. Baud rate _____.
9. CISCO 2511 userid and password_____.
10. **EM Client ONLY**
    Socket numbers of the host EM Server: _____.

14.3 Installing and Configuring Remote Standalone

14.3.1 Core segments

Prior to loading any GCCS software segments on your workstations, review the section on Segment Installation of the GCCS System Administration Manual. Use of the Segment Installer is explained in depth. If you are building this remote workstation at a host site, you can take advantage of the network installation servers rather than load from tape. You must ensure that you mount the */h/data/global/SysAdm* directory from the 'Emserver' on this workstation:

mount <emserver name/ip address>:/h/data/global/SysAdm /data/global/SysAdm

Install all segments listed in the table and follow the instructions listed in Comments field.

Table 14.3.1-1. Core Segments for Remote Platforms

Application	Version	Size	Tape	Comments
Applix	3.2	92379	2.2 (AP.1)	Must be loaded before Command Center Apps
ASET Server	gv.1.02	25	2.2 (AP.2)	
Auditing	3.0.04	112	2.2 (AP.1)	Load BSM Patch 1 before deinstalling old Auditing.
EM Patch	6.0.1	22462	2.2 (AP.1)	Load only on an upgrade from 2.1 to 2.2.
EM Printer Admin	2.3.1.04	3084	2.2 (AP.1)	
filemgr	1.0	19	2.2 (AP.1)	
GCCS COE	2.2.0.5.02	68153	2.2 (AP.1)	Reboot Workstation after loading.

GCOEPTC	1.0.02		2.2.2 (UP.1)	
Kernel Patch 3	1.5	309	2.2.1 (AP.1)	Must reboot after loading.
GCCS ftptool	4.3	342	2.2 (AP.1)	
ICON FOR APPLIX	1.0	21	2.2 (AP.1)	Install if not using Sybase
PERL	6.0	4720	2.2 (AP.1)	
Remote Access	1.2	1624	2.2 (AP.1)	Install last, refer to instructions below for installing!
Remote Install	1.1.1	2068	2.2 (AP.1)	
System Maintenance	2.2	421	2.2.1 (UP.1)	
Tcl/Tk	1.0.0	10504	2.2.2 (AP.1)	
UPSI Power Monitor	1.3b	441	2.2 (AP.1)	Cable must be connected prior to installation. Load only if using UPSI system.
XLOCK ICON	1.0	21	2.2 (AP.1)	

NOTE: You may wish to install any other segments on this workstation prior to installation of the Remote Access segment, since it reconfigures the workstation's Ethernet ports.

14.3.2 Remote_Access Segment

The following are the steps for installing the Remote Access segment. Load the segment with the SAInstaller. See Table 14.3.2-1.

Table 14.3.2-1. GCCS Remote Connectivity Segment

Application	Version	Size	Tape	Comments
Remote Connectivity Segments				
Remote Access	1.2		2.2 (AP.1)	

WARNING: Do not install **REMOTE_ACCESS** on anything other than a remote SPARCstation. Installation disables the SPARCstation's Ethernet ports, allowing only PPP dial-up network access. Once installed, a complete reinstallation of the Operating System and all GCCS components will be required in order to restore use of the Local Area Network (LAN) Ethernet ports!

WARNING: Among the many files installed in this step is */etc/asppp.cf*. This file contains a debug parameter which defines the amount of diagnostics information is provided during a connection.
Changing this parameter can be useful, when debugging a connection problem, in order to provide additional diagnostics information. Do not arbitrarily change this parameter - it should be left at its default (currently, 4). Should you change it, be sure to change it back to its original value.
REMINDER: Only edit this file when directed to do so by knowledgeable Solaris PPP experts who are attempting to debug a connection problem.

The following are a list of questions that the installer must answer to complete the installation this segment:

```
Do you wish to continue the installation of this Remote Access (y/n) [n]:
```

1. Enter [**Y**] and press the <**Return**> key.

```
Do you want to continue with the installation of <SUNWapppr> [y or n]
```

2. Enter [**Y**] and press the <**Return**> key.

```
Do you want to install these as setuid/setgid files [y/n or q]
```

3. Enter [**Y**] and press the **<Return>** key.

```
Do you want to continue with the installation of <SUNWbnuu> [y or n]
```

4. Enter [**Y**] and press the **<Return>** or **<Enter>** key.

```
Do you want to continue with the installation of <SUNWbnur> [ y or n]
```

5. Enter [**Y**] and press the **<Return>** or **<Enter>** key.

```
Press <cr> to continue
```

6. Press the **<Return>** or **<Enter>** key.

```
What is the PPP configuration of this workstation?
        a)      Standalone EM Server workstation, infrequent use of PPP
        b)      EM Client, PPP connection always up
```

7. Enter [**a**] and press the **<Return>** or **<Enter>** key.

```
Enter the Ethernet IP Address of the Cisco 2511 COMM SERVER: _____
```

8. Enter **IP Address** and press the **<Return>** or **<Enter>** key.

```
Enter the IP Address of the APPLICATIONS SERVER: _____
```

9. Enter **IP ADDRESS** and press the **<Return>** or **<Enter>** key.

```
Enter the IP Address to user for the PPP connection: _____
```

10. Enter **IP Address** and press the **<Return>** or **<Enter>** key.

```
Enter the SERIAL PORT the modem is connected to ('a' or 'b'): __
```

11. Enter [**a** or **b**] and press the **<Return>** or **<Enter>** key. It is important that you physically verify which serial port is connected to the STU-III. Look at the back of the SPARCstation - each serial port is labeled below the serial connector, "Serial A" (on the right, when facing unit from the rear) and "Serial B" (on the left, when facing unit from the rear).

```
Enter the connection type:
        a) STU-III modem
        b) Direct connect to communications server
```

12. Enter the correct response for your site and press the **<Return>** or **<Enter>** key.

NOTE: If your site has direct connection, you will not be prompted for the telephone number of the communications server.

```
Enter the TELEPHONE NUMBER OF THE COMMUNICATIONS SERVER: ,_________
```

13. Enter telephone number of the communications server, for STU-III connection only, with a leading ',' (e.g., **,7037358882**) and press the **<Return>** or **<Enter>** key.

```
Enter the serial port BAUD Rate (9600 19200 38400): _____________
```

14. Enter the baud rate for your workstation's serial port (ie., the rate at which your serial port connects to your modem, STU-III, MUX or direct line - should be set at the same rate as the device to which you connect, **38400** is recommended) and press the **<Return>** or **<Enter>** key.

NOTE: The configuration information that was entered will be displayed for validation. If correct enter [**Y**] otherwise, enter[**N**] and re-enter the correct information.

Is the above information correct (y/n)? __

15. Enter [**Y**] and press the **<Return>** or **<Enter>** key.

Installation completed, please REBOOT the system. Press **<Return>** to continue..

16. Press the **<Return>** or **<Enter>** key and the workstation will re-boot.

14.4 Installing and Configuring Remote EM_Client

14.4.1 Core segments

Prior to loading any GCCS software segments on your workstations, review the section on Segment Installation of the GCCS System Administration Manual. Use of the Segment Installer is explained in depth. If you are building this remote workstation at a host site, you can take advantage of the network installation servers rather than load from tape. You must ensure that you mount the /h/data/global/SysAdm directory from the 'Emserver' on this workstation:

mount <emserver name/ip address>:/h/data/global/SysAdm /data/global/SysAdm

Install all segments listed in Table 14.3.1-1 and Table 14.3.2-1 and follow the instructions listed in Comments field.

NOTE: You may wish to install any other segments on this workstation prior to installation of the Remote Access segment, since it reconfigures the workstation's Ethernet ports.

14.4.2 Remote_Access Segment (EM_Client)

The following are the steps for installing the Remote Access segment. Load the segment with the SAInstaller.

W
ARNING: Do not install **REMOTE_ACCESS** on anything other than a remote SPARCstation. Installation disables the SPARCstation's Ethernet ports, allowing only PPP dial-up network access. Once installed, a complete reinstallation of the Operating System and all GCCS components will be required in order to restore use of the Local Area Network (LAN) Ethernet ports!

W
ARNING: Among the many files installed in this step is */etc/asppp.cf*. This file contains a debug parameter which defines the amount of diagnostics information is provided during a connection. Changing this parameter can be useful, when debugging a connection problem, in order to provide additional diagnostics information. Do not arbitrarily change this parameter - it should be left at its default (currently, 4). Should you change it, be sure to change it back to its original value.
REMINDER: Only edit this file when directed to do so by knowledgeable Solaris PPP experts who are attempting to debug a connection problem.

The following are a list of questions that the installer must answer to complete the installation this segment:

Do you wish to continue the installation of this Remote Access (y/n) [n]:

1. Enter [**Y**] and press the **<Return>** key.

Do you want to continue with the installation of <SUNWapppr> [y or n]

2. Enter [**Y**] and press the **<Return>** key.

Do you want to install these as setuid/setgid files [y/ n or q]

3. Enter [**Y**] and press the **<Return>** key.

Do you want to continue with the installation of <SUNWbnuu> [y or n]

4. Enter [**Y**] and press the **<Return>** or **<Enter>** key.

Do you want to continue with the installation of <SUNWbnur> [y or n]

5. Enter [**Y**] and press the **<Return>** or **<Enter>** key.

Press <cr> to continue

6. Press the **<Return>** or **<Enter>** key.

What is the PPP configuration of this workstation? a) Standalone EM Server workstation, infrequent use of PPP b) EM Client, PPP connection always up

7. Enter [**b**] and press the **<Return>** or **<Enter>** key.

Enter the Ethernet IP Address of the Cisco 2511 COMM SERVER: _____

8. Enter [**Y**] and press the **<Return>** or **<Enter>** key.

Enter the IP Address of the APPLICATIONS SERVER: _____

9. Enter **IP ADDRESS** and press the **<Return>** or **<Enter>** key.

Enter the IP Address to user for the PPP connection: _____

10. Enter **IP Address** and press the **<Return>** or **<Enter>** key.

Enter the SERIAL PORT the modem is connected to (‘a’ or ‘b’): __

11. Enter [**a** or **b]** and press the **<Return>** or **<Enter>** key. It is important that you physically verify which serial port is connected to the STU-III. Look at the back of the SPARCstation - each serial port is labeled below the serial connector, "Serial A" (on the right, when facing unit from the rear) and "Serial B" (on the left, when facing unit from the rear).

```
Enter the connection type:
        a) STU-III modem
        b) Direct connect to communications server
```

12. Enter the correct response for your site and press the **<Return>** or **<Enter>** key.

NOTE: If your site has direct connection, you will not be prompted for the telephone number of the communications server.

```
Enter the TELEPHONE NUMBER OF THE COMMUNICATIONS SERVER: ,_________
```

13. Enter telephone number of the communications server, for STU-III connection only, with a leading ',' (e.g., **,7037358882**) and press the **<Return>** or **<Enter>** key.

```
Enter the serial port BAUD Rate (9600 19200 38400): _____________
```

14. Enter the baud rate for your workstation's serial port (ie., the rate at which your serial port connects to your modem, STU-III, MUX or direct line - should be set at the same rate as the device to which you connect, **38400** is recommended) and press the **<Return>** or **<Enter>** key.

NOTE: The configuration information that was entered will be displayed for validation. If correct enter [**Y**] otherwise, enter[**N**] and re-enter the correct information.

```
Is the above information correct (y/n)? __
```

15. Enter [**Y**] and press the **<Return>** or **<Enter>** key.

```
Installation completed, please REBOOT the system.
Press <Return> to continue..
```

16. Press the **<Return>** or **<Enter>** key and the workstation will re-boot.

14.5 Login to Remote Platforms

14.5.1 Standalone

In order to use a standalone workstation, there should be a local login account for a user and a character based login account at the host site. A user will login at the GCCS globe login screen and will be presented with a desktop with two icons, labeled "Control" and "Access". These two programs offer the user the means of accessing the host site's GCCS suite.

The "Control" icon establishes the communication link with the host site's server. The user will be prompted for a user-id and password for the CISCO 2511 router. This information is available from the router administration staff. The "Access" icon establishes a terminal session with the host server after the communications link is established. The user will be presented with an 'xterm session' window that the user will key in the appropriate login for the host site's server. The user will then be presented with a menu of character based applications that the user is authorized to use. The user will use the "Tab" key to maneuver through the menu to select an application to use and then press the <**Return**> or <**Enter**> key to activate the application.

14.5.2 EM_Client

14.5.2.1 Booting and Login of EM_Client Workstation

When a remote workstation that has been configured as an "em_client" is booted, the PPP software automatically establishes the communications link with the host site. The workstation will prompt for 'username' and 'password' information of an account on the Cisco 2511 Remote Access Server. After this information is entered, a line of dots will be drawn, and beeps will sound, while the workstation establishes a connection to the Cisco 2511 Remote Access Server. Once the connection is complete, the system will finish booting.

14.5.2.2 Initial Configuration of EM_Client Workstion

Perform the following steps:

1. Logon to the globe as sysadmin. You must take the following corrective steps:

2. Edit **[vi]** the **/etc/resolv.conf** file. Verify that a fully qualified domain name is contained in this file (e.g., bur.osf.disa.mil). This information is entered when Solaris is installed - improperly entering this information at that time will lead to the system being in **DEGRADED** mode.

3. Edit **[vi]** the **/etc/services** file. Change the LAN SEGID to mat that of the EM server at the host site. Write down the lines that contain **udp** under the **# GCCS Exec Mgr Services** section of this file.

Edit **[vi]** the **/etc/services** file on the machine you are configuring.
Scroll down approximately 85% through the document until you reach lines that look like this:

GCCS Exec Mgr Services
u6sysexec nnnnn/udp

Change the lines containing **ud**p under the **# GCCS Exec Mgr Services** section of this file so that the **nnnnn** entries match those of the EM Server.

4. Edit **[vi]** the **/etc/netmasks** file. Change the netmask as follows:
Determine the IP address of the host site's EM Server (e.g., 164.117.208.227),
Change the netmask in the **/etc/netmasks** file to be the address from the previous step, but with the fourth octet changed to a zero (e.g., 164.117.208.0). Edit **[vi]** the **/etc/networks** file. Change the **SUBNET1.GCCS** to the IP address of the EM Server (e.g., 164.117.208.227).

5. Logon to the **'root**' account and execute a '**ping**' of the EM Server. If this completes without error, the workstation can be initialized as a NIS+ client:

6. Edit **[vi]** the **/etc/hosts** file. Add an alias of the host site's EM Server to **emserver**.

7. Initialize NIS+. See the Systems Administration Manual, GCCS version 2.1, section 6.2.3, for the procedure for initializing a workstation on an Ethernet LAN as a NIS+ client.

8. After NIS+ reboot, login as **sysadmin**, and do the following:

   Open an X-Term window and execute the following commands:

   # **cd /h/REMOTE_ACCESS**
   # **/h/EM/progs/load_profiles data/Profiles/Profiles.RA**

   Add additional Application Server entries, if desired. The IP address/hostname pairs must be added to the **/etc/hosts** file, and the host names added to the **/h/REMOTE_ACCESS/data/config/apps_hosts** file.

14.5.3 Debugging and Modifying Configuration

14.5.3.1 Incorrect Serial Port

WARNING: It is important that you physically verify which serial port is connected to the STU-III. Look at the back of the SPARCstation - each serial port is labeled, directly below the serial connector, "Serial A" (on the right, when facing unit from the rear) and "Serial B" (on the left, when facing unit from the rear).

Failure to enter the correct serial port identifier [a or b] will result in not being able to connect to the host site.

Should you incorrectly enter the serial port identifier, or later choose to physically reconfigure which serial port is used (the latter is not recommended), you can manually reconfigure REMOTE_ACCESS to specify the serial port to use. Perform these recovery actions:

a. Logon as **root**

b. Edit **[vi]** the file **/etc/uucp/Devices.ra-ppp**

1. The last two lines of this file should look as follows (assuming port 'a' was selected):

   ACU cuaa - 38400 stu
   Direct cuaa - 38400 direct

2. Change the letter immediately following "cua" on each line (e.g.., the 'a') to the port ID you wish to use (e.g., 'b'):

   ACU cuab - 38400 stu
   Direct cuab - 38400 direct

c. Reboot

NOTE: Should you incorrectly enter the phone number, or later choose to change the phone number used (the latter is not recommended), you can manually reconfigure REMOTE_ACCESS to specify the phone number to use.

Reminder: Only edit this file as a last resort if you have incorrectly entered your port ID.

14.5.3.2 Incorrect Telephone Number for STU-III

Perform these actions:

1. Logon as ***root***

2. Edit **[vi]** the file **/etc/uucp/Systems.master**
   Change the phone number, as appropriate.

3. **Reboot.** See system reboot instructions in section 3.3.1, *How to reboot a Sun workstation.*, on page 4.

REMINDER: Only edit this file if you have incorrectly entered the phone number to be called.

14.5.3.3 Unable to Connect to Host Site

Should you be unable to connect to the host site, despite all parameters and configuration items being correct [**PLEASE CHECK**], the CISCO 2511 router at the host site may need to be restarted. Only perform these actons if unable to connect and all other corrective actions have failed.

SECTION 15. LOADING GCCS MISSION APPLICATIONS

15.1 GCCS Mission Applications of all Non-JOPES Applications Excluding UB.

Table 15-1 list GCCS Mission Application segments that may be loaded on a application server, client, or Oracle database server. The segments are listed in alphabetic, key points regarding installation are listed below:

1. JDISS Server must be loaded before JDISS Client or JDISS Image Product Archieve

2. Those applications that have database server segments on the database tape will require Oracle Apps Server Tools on the Application server.

3. AMHS Client requires TOPIC. When loading the AMHS segments the AMHS Installation Procedures should be consulted.

Table 15-1. GCCS Mission Applications

Application	Version	Size	Tape	Comments
AMHS Segments				
AMHS Client	3.1.2.01		2.2 (AP.1)	
AMHS Server	2.1.4	11155	2.2 (AP.2)	
AMHS Server Patch	3.1.2.01		2.2 (AP.2)	
COTS Topic	3.1.5c		2.2 (AP.1)	
JOPES Application Segments				
Oracle Application Server Tools	7.1.4.06		2.2 (AP.1)	
Non-JOPES Mission Applications				
AirFields	2.1.2		2.2 (AP.2)	
AirFields Remote	1.0.01		2.2 (AP.1)	
EVAC Client	2.3.01	24147	2.2.2 (AP.1)	
FRAS SUPPORT	1.2.6		2.2 (AP.1)	
FRAS SUPPORT Remote Client	1.2.6.01		2.2 (AP.1)	
GCCS ATO Review Capability	1.0.1	5567	2.2 (AP.1)	

Table 15-1. GCCS Mission Applications (Cont.)

GCCS ATO Rev Cap Patch	1.0.0		2.2 (AP.1)	
Global Reconnaisance Informtion System Core	2.3.2.02		2.2.1 (UP.1)	
JDISS Client	2.0.4.01		2.2 (AP.1)	
JDISS Server	2.0.3.01		2.2 (AP.2)	
Target Multimedia Tool	2.2.2.06		2.2 (AP.2)	
Non-JOPES Oracle Database Segments				
FRAS SUPPORT for Database Access	1.2.1		2.2 (DB.1)	
GRIS Database Server	1.0.02		2.2 (DB.1)	